

CLAIMS

What is claimed is:

1. A method of verifying a user in a health-related transaction, the method comprising:
 - receiving a request from a portable healthcare device to perform a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site;
 - receiving biometric data from the portable healthcare device;
 - determining whether corresponding biometric data is stored;
 - if corresponding biometric data is stored, determining validity of credential information associated with a user; and
 - if the credential information is valid, sending to the portable healthcare device, enabling information for performing the health-related transaction.
2. The method of claim 1, wherein the request includes login information to initiate a session and the enabling information includes session information.
3. The method of claim 2, wherein the determining of validity of credential information includes sending a request for a credential check to a credential service and receiving a credential check result from the credential service.

4. The method of claim 2, further including requiring the login information after a pre-designated time period of inactivity.

5. The method of claim 1, wherein the enabling information includes the credential information for forwarding to the remote information site.

6. The method of claim 5, wherein the determining of validity of credential information includes comparing the credential information to previously determined credential information for a current session.

7. The method of claim 1, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data.

8. The method of claim 1, wherein if corresponding biometric data is not stored, further including denying the requested health-related transaction.

9. The method of claim 1, wherein the receiving biometric data occurs at pre-designated intervals of time.

10. A system for verifying a user in a health-related transaction, comprising:

- a) a biometric database to store biometric data;
- b) a biometric engine to determine whether corresponding biometric data is stored in the biometric database for a user of a portable healthcare device requesting a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site;
- c) a credential request unit to determine validity of credential information associated with the user if corresponding biometric data is stored; and
- d) an internal network port to receive the request for the health-related transaction from the portable healthcare device and to send enabling information for performing the health-related transaction to the portable healthcare device if the credential information is valid.

11. The system of claim 10, wherein the request includes login information to initiate a session and the enabling information includes session information

12. The system of claim 11, further including an external network port to send a request for a credential check from the credential request unit to a credential service and receive a credential check result from the credential service.

P00000000000000000000000000000000

13. The system of claim 10, further including a notification unit to send a requirement for the login information after a pre-designated time period of inactivity.
14. The system of claim 10, wherein the enabling information includes the credential information for forwarding to the remote information site
15. The system of claim 14, wherein the credential request unit is to compare the credential information to previously determined credential information for a current session.
16. The system of claim 10, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data.
17. A computer accessible medium having stored therein a plurality of sequences of executable instructions, which, when executed by a processor, cause the system to:

receive a request from a portable healthcare device to perform a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site;

receive biometric data from the portable healthcare device;

determine whether corresponding biometric data is stored;

if corresponding biometric data is stored, determine validity of credential information associated with a user; and

if the credential information is valid, send to the portable healthcare device, enabling information for performing the health-related transaction.

18. The computer accessible medium of claim 17, wherein the request includes login information to initiate a session and the enabling information includes session information.
19. The computer accessible medium of claim 18, wherein the determining of validity of credential information includes sending a request for a credential check to a credential service and receiving a credential check result from the credential service.

PCT/US2016/035660

- 20. The computer accessible medium of claim 18, further including additional sequences of executable instructions, which, when executed by the processor further cause the system to require the login information after a pre-designated time period of inactivity.
- 21. The computer accessible medium of claim 17, wherein the enabling information includes the credential information for forwarding to the remote information site.
- 22. The computer accessible medium of claim 21, wherein the determining of validity of credential information includes comparing the credential information to previously determined credential information for a current session.
- 23. The computer accessible medium of claim 17, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data
- 24. The computer accessible medium of claim 17, further including additional sequences of executable instructions, which, when executed by the processor

further cause the system to interrupt a processor to deny the requested health-related transaction if corresponding biometric data is not stored.

25. The computer readable medium of claim 17, wherein the receiving biometric data occurs at pre-designated intervals of time.
26. A method of verifying a user in a health-related transaction, the method comprising:

receiving a request from a portable healthcare device to perform a health-related transaction in real-time across a network pathway from the portable healthcare device to a remote information site, the request including login information to initiate a session;

receiving biometric data from the portable healthcare device;

determining whether corresponding biometric data is stored;

if corresponding biometric data is stored, determining validity of credential information associated with a user comprising sending a request for a credential check to a credential service and receiving a credential check result from the credential service; and

if the credential information is valid, sending to the portable healthcare device, enabling information for performing the health-related transaction including session information for performing the health-related transaction.

27. The method of claim 26, further including requiring the login information after a pre-designated time period of inactivity.
28. The method of claim 26, wherein the enabling information includes the credential information for forwarding to the remote information site
29. The method of claim 26, wherein the biometric data includes voice data, digital electronic signature data, fingerprint image data, or eye image data.